

FILED

JUN - 9 2017

CLERK, U.S. DISTRICT COURT  
NORFOLK, VA

**UNITED STATES DISTRICT COURT**  
 for the  
 Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

)

Case No. 4:17 SW30

Instagram Account(s) associated with usernames  
"bigmoney\_jordan," "freebandkid23," and  
"freebandservo," as detailed in Attachment A

)

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §1349	Conspiracy to Commit Bank Fraud
18 U.S.C. § 1344	Bank Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

See affidavit.

Continued on the attached sheet.

Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

*Kaitlin C. Graton*

Kaitlin C. Graton

Assistant United States Attorney



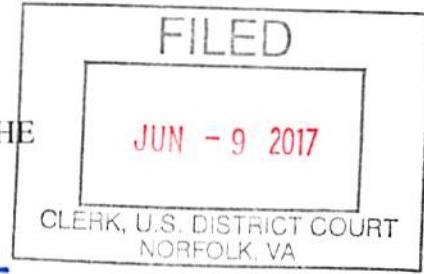
Derek M. Mullins, United States Postal Inspector  
 Printed name and title

Sworn to before me and signed in my presence.

Date: June 9, 2017City and state: Norfolk, Virginia


The Honorable Robert J. Krask U.S. Magistrate Judge  
 Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA



IN RE SEARCH OF

) ~~80~~ UNDER SEAL

)  
INFORMATION ASSOCIATED )  
WITH INSTAGRAM, INC. ACCOUNT(S) )  
ASSOCIATED WITH USERNAMES )  
“BIGMONEY\_JORDAN” )  
AND “FREEBANDKID23” )  
AND “FREEBANDSWERVO” )  
THAT IS STORED AT )  
PREMISES CONTROLLED BY )  
INSTAGRAM )

4.17-mj- 4:17sw30

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Derek Mullins, being duly sworn, hereby depose and state:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Instagram, Inc. (“Instagram”), a social-networking company headquartered in San Francisco, California and owned by Facebook, Inc., a social-networking company headquartered in Menlo Park, California, as described in Attachment A. The information to be searched is described in the following paragraphs and in Attachment B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Instagram to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Instagram accounts described in Attachment A. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (“USPIS”). I have been employed as a Postal Inspector since April 2015. Prior to becoming a Postal Inspector I was employed by the Department of Homeland Security, Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”) since August 2008. I am a graduate of the Federal Law Enforcement Training Center’s Criminal Investigators Training Program and the U.S. Immigration and Customs Enforcement Academy’s ICE Special Agent Training Program. Prior to my employment with HSI, I was a Deputy Sheriff with the Wise County Sheriff’s Department in Wise County, Virginia from 2005 to 2008. I have received training in various aspects of federal law enforcement including the investigation of identity theft, fraud, and narcotics related offenses, as well as numerous other federal and state offenses. I have participated in multiple investigations, seizures, and search warrants, which have resulted in criminal arrests, seizures, and prosecutions. I have also been the affiant on search, arrest, and seizure warrants that have resulted in successful arrests, seizures, and prosecutions.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1349 (Conspiracy to Commit Bank Fraud), 1344 (Bank Fraud), and 1028A(a)(1) (Aggravated Identity Theft) have been committed by Markis Dickerson (“DICKERSON”), Christopher BOONE (“BOONE”), and other

persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes and items to be seized listed in Attachment B.

**RELEVANT STATUTES**

5. Title 18, United States Code, Sections 1349 prohibits any person from “attempt[ing] or conspir[ing] to commit any offense under this chapter.” Sections 1344 is contained in the same chapter.

6. Title 18, United States Code, Sections 1344 prohibits anyone from “knowingly execut[ing], or attempt[ing] to execute, a scheme or artifice—(1) to defraud a financial institution; or (2) to obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations or promises.”

7. Title 18, United States Code, Section 1028A prohibits anyone, during and in relation to any enumerated felony violation, from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. Title 18, United States Code, Section 1028A enumerates felony violations, including any provision contained in chapter 63 (relating to mail, bank, and wire fraud).

**PROBABLE CAUSE**

8. In December 2014, I became involved in an investigation into a group of individuals who were using financial institutions to negotiate fraudulent assets into cash withdrawals from ATMs. The fraud scheme began in or about August 2014 and involved the suspects soliciting current bank accountholders on social media sites, including Facebook and Instagram. At the suspects’ direction and in exchange for promise of payment, the accountholders would provide their debit/credit cards and PIN numbers. The suspects would

then deposit worthless or stolen checks into the compromised accounts using various ATMs in the Hampton Roads area of Virginia. Once the checks were deposited at an ATM, the bank of deposit credited the account of deposit with all or some of the check's stated value. The suspects would then make ATM withdrawals and conduct other transactions to access the maximum allowable amount each day the account was used in the scheme. When the suspects were conducting the fraudulent withdrawals or deposits, the financial institutions had cameras recording the transactions.

9. During this investigation, Markis Jordan DICKERSON ("DICKERSON") was identified, through interviews of accountholders and debriefs of defendants, as one of the individuals conducting this scheme, alone and with others, throughout the Hampton Roads area of Virginia.

10. As part of this investigation, investigators were able to view some of DICKERSON'S publicly available activity on Facebook and Instagram. Investigators saw numerous photographs of DICKERSON holding large quantities of cash, debit/credit cards, firearms, narcotics, and ATM receipts. Investigators also identified conversations on DICKERSON'S social media accounts in which DICKERSON was soliciting accountholders for their debit/credit cards to engage in the fraud scheme. For example, investigators identified a January 2015 Facebook conversation between DICKERSON and C.W. in which DICKERSON messaged C.W. and stated, "If you got a bank account and you trynna make a couple thousand let me know." During this conversation, DICKERSON explained to C.W. how to set up a bank account and provide the "bank card" and "4 digit PIN." DICKERSON further explained that he has been able to take "official bank business checks" and "deposit 5 racks in one account."

11. In addition to these conversations, on January 22, 2015, a state search warrant was executed on an iPhone 5C bearing serial number: C7KLLA31FFHH belonging to DICKERSON. During the search of the phone, investigators located numerous photographs depicting bank receipts; debit cards; and DICKERSON posing with large sums of U.S. currency, firearms, and narcotics. Specifically, one photograph depicted two Bayport Credit Union receipts dated December 11, 2014. Both receipts showed the last four digits of the account number. One of the receipts showed a balance of \$5514.51 and the second showed a balance of \$5625. Five photographs of debit cards bearing names other than DICKERSON's were identified. There was also an "account snapshot" of a Langley Federal Credit Union ("LFCU") account issued to an individual named E.B. The snapshot depicts a balance of \$6,089 on December 18, 2014 and returned deposit check for -\$6,084 on December 30, 2014. There was also a photograph of DICKERSON standing with a stack of U.S. currency against his ear, as if he were talking on a telephone, and holding a black handgun with an extended magazine in the other hand.

12. As a result of the 2014 investigation, four individuals were charged and convicted in the Eastern District of Virginia of conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1). *United States v. Frazier et al.*, 4:15cr43. DICKERSON was not charged in the original investigation.

13. In approximately December 2016, I was contacted by an LFCU fraud investigator requesting assistance with an investigation that involves DICKERSON, Christopher Douglas BOONE ("BOONE"), and others concerning the use of LFCU and other financial institutions to negotiate worthless and counterfeit financial instruments into U.S. currency and other instruments. The investigator indicated that LFCU had discovered numerous transactions in multiple LFCU accounts involving the deposit of fraudulent checks and money orders and

subsequent withdrawal and use of the funds credited on such deposits. LFCU had also identified purchases of money orders from retail locations through which DICKERSON, BOONE, and others obtained the cash value of the fraudulently deposited instruments. LFCU had identified and preserved video and still surveillance images of DICKERSON, BOONE, and others conducting the transactions.

14. LFCU is a federally insured financial institution, as defined in 18 U.S.C. § 20.

15. The LFCU investigator was able to identify and interview numerous accountholders whose accounts had been used to effect the fraudulent transactions. According to the LFCU investigator, many accountholders reported that DICKERSON and others had contacted them via social media outlets to solicit their banking information. Specifically, DICKERSON and others first posted a public message seeking accountholders interested in making money. DICKERSON and others would then send private or direct messages to those who responded positively to the public message. In these private and direct messages, DICKERSON and others generally requested that all further communications be conducted via text messages or telephone calls. DICKERSON and others then directed accountholders to provide their debit cards and PINs to DICKERSON, BOONE, and others. DICKERSON and others arranged to meet accountholders at various locations to obtain debit cards and PINs, promising to deposit money into the accounts associated with such debit cards. DICKERSON, BOONE, and others then used those debit cards and PINs to effect deposits of worthless and counterfeit financial instruments, including checks and money orders, into the associated accounts. Once funds were credited to those accounts, DICKERSON, BOONE, and others used the associated debit cards and PINs to withdraw U.S. currency from ATMs and to make purchases at retail locations.

16. Debit card numbers and PINs are means of identification, as defined in 18 U.S.C. § 1028(d)(7), for the accountholders to which they are assigned. Based on information gathered during the course of this investigation, I have identified three usernames associated with the Instagram account that DICKERSON has used to solicit and communicate with accountholders and others in furtherance of the scheme. These are usernames “bigmoney\_jordan” and/or “freebandkid23” and/or “freebandswervo.”

17. As part of this investigation, I have reviewed additional postings and messages made to and through Instagram and Facebook accounts in which DICKERSON and others have discussed and attempted to further the scheme. The following are examples of such postings:

- a. During the execution of a state search warrant on a Facebook account belonging to D.G., an associate of DICKERSON, investigators identified an October 31, 2016 series of direct messages between D.G. and DICKERSON concerning the scheme. DICKERSON was using the Facebook account located at <http://www.facebook.com/markis.jordan.7>, which was then listed under the username “Freeband Jordan.” That account is currently listed under the username “Lee Swervo.”

In the October 31, 2016 conversation, D.G. asked DICKERSON to explain “dat money train.” DICKERSON responded, “Gotta find people wit bank accounts.” D.G. stated that “presto” had been telling him/her to “get on that shit the other day navy and langly.” DICKERSON responded, “Yea shit crazy we was all gettin money out here before him and Ki Ki got locked but they was droppin fake checks and sometimes it would clear but I ran into da plug himself he make the official shit on his laptop and everything it ain’t no where near how we used to do it.”

As a result of the 2014 investigation, I know that “presto” is a nickname used by Preston Frazier and “Ki Ki” is a nickname used by Keandre Williams. Both of these individuals were prosecuted and convicted in that investigation. See *United States v. Frazier et al.*, 4:15cr43.

- b. In December 2016, investigators were monitoring DICKERSON’s public Instagram account, then associated with the username “freebandkid23.” Investigators observed an image posted to that account depicting an LFCU account overview, as it would appear when the account is accessed through an online banking application. The overview includes the Smart Checking and Savings accounts belonging to H.B., an accountholder investigators have

associated with the current scheme. This screenshot was posted along with the following message: "Who got Langley and want 3800 in their account by tomorrow morning???"

- c. In February 2017, investigators were again monitoring DICKERSON's public Instagram account. At that time, the account was associated with the user name "freebandserv." The account appeared to be the same account previously associated with the username "freebandkid23."<sup>1</sup> Investigators observed an image posted to that account depicting a USAA account overview, as it would appear when the account is accessed through an online banking application. The overview includes a Classic Checking account belonging to H.F., another accountholder investigators have associated with the current scheme. The balance of the account was then \$4,643.65. This screenshot was posted along with the following message: "Had me a good ol morning . . . HIT ME UP IF YOU WANT SOME MONEY IN YOUR ACCOUNT TODAY!!" In the days that followed this posting, investigators observed additional postings of screenshots depicting the same account with a higher available balance. One such posting showed a current balance of \$12,759.24 and included the following messages: "Who want at least 4,000 in their account?" and "If you want at least 4,000 in your account DM me."
- d. Also in February 2017, investigators observed an image posted to DICKERSON's public Instagram account, also made when the account was associated with the username "freebandserv." That image depicted the same LFCU account overview for the account belonging to H.B., which investigators had previously observed in December 2016. This screenshot was re-posted along with the following message: "If you have Langley and want 3800 in your account DM me ASAP." Several Instagram users responded to the public post. DICKERSON replied on three occasions to these users advising them to contact him on his posted telephone number.

18. As part of this investigation, I have reviewed police reports filed by accountholders concerning their contact with DICKERSON and others. The following are examples of such reports:

- a. According to a Newport News Police report, on or about January 6, 2017, DICKERSON contacted K.S. via social media and requested to use his/her bank account, purportedly because he was not able to access his own account. K.S. advised he/she "thought he was going to pay" him/her to use his/her bank account. They met and DICKERSON provided K.S. with two personal checks from his old account and requested he/she deposit them into his/her account. K.S. also gave DICKERSON his/her debit card and PIN. K.S. deposited the checks as requested and notified DICKERSON. K.S. was later

---

<sup>1</sup> Investigators have also associated the username "bigmoney\_jordan" with that same account.

contacted by his/her bank indicating that the checks he/she had deposited were fraudulent. K.S.'s bank further advised that additional counterfeit checks had been deposited into the account and cash withdrawals had been made at various ATMs, causing the account to be overdrawn. The bank also notified K.S. that a large purchase was made at Walmart. On January 30, 2017, Detective E. Benson met with the Asset Protection Manager at Walmart and viewed the surveillance video of the transaction described above. Detective E. Benson positively identified DICKERSON as the individual making the transaction.

- b. According to a Hampton Police report, on or about January 17, 2017, DICKERSON contacted E.L. via social media and indicated that he could "make [him/her] some money." According to the police report, DICKERSON deposited four counterfeit checks into E.L.'s account totaling \$3,853.43. After the money was deposited, DICKERSON contacted E.L. to obtain the online username and password for his/her LFCU account. DICKERSON advised he needed to login to the account and see if the money was available. DICKERSON also stated he needed to physically obtain E.L.'s debit card and PIN to ensure E.L. would "not go to the bank and steal all the money." On January 17, 2017, DICKERSON drove to E.L.'s residence and retrieved his/her debit card and PIN. On January 18, 2017, E.L. contacted LFCU and discovered that \$500 had been withdrawn from the account via ATM. E.L. stated there were no funds in his/her account prior to DICKERSON depositing the counterfeit checks.

19. From approximately at least December 2016 through April 13, 2017, DICKERSON, BOONE, and others have participated in ATM transactions on more than 45 accounts issued by LFCU, SunTrust Bank ("SunTrust"), 1<sup>st</sup> Advantage Federal Credit Union ("1<sup>st</sup> Advantage"), and other financial institutions, all of which are federally insured financial institutions, as defined in 18 U.S.C. § 20. In each of these transactions, U.S. currency was withdrawn following the deposit of a worthless or counterfeit financial instrument via "remote capture deposit." A "remote capture deposit" is a deposit accomplished through the transmission of information to the institution of deposit via a mobile application on an electronic device with either cellular or internet access. During each of the withdrawals that followed such deposits, DICKERSON and BOONE were captured by ATM surveillance equipment either personally conducting the transaction or accompanying the individual(s) who conducted the transaction.

9

*pje*

*DWU*

Through review of LFCU's records and its interviews with actual accountholders, investigators have determined that during the period of time surrounding these transactions, the individual through whose account the transaction was done had telephonic contact with DICKERSON and/or BOONE.

20. The following are examples of the transactions identified to date as being associated with DICKERSON and BOONE:

- a. On December 13, 2016, three fraudulent checks were deposited into K.M.'s LFCU account via remote capture deposit. On the same day, four transactions were attempted/conducted at an LFCU branch located on West Mercury Boulevard in Hampton, Virginia. The first transaction was an attempted ATM withdrawal at the drive-thru ATM using K.M.'s debit card and PIN. BOONE was captured by the ATM's surveillance equipment driving a black car through the drive-thru ATM and attempting to withdraw \$500 from K.M.'s account at that ATM. After the transaction was declined, BOONE then attempted a second successful withdraw of \$300 from K.M.'s account. DICKERSON was captured by the ATM's surveillance equipment in the passenger seat beside BOONE during these transactions. Approximately two minutes after BOONE drove away from the ATM, DICKERSON was captured by the walk-up ATM's surveillance equipment conducting two separate withdrawals; each for \$100. K.M.'s debit card and PIN were used during each of these transactions.
- b. On January 26, 2017, three counterfeit checks were deposited into J.B.'s LFCU account via remote capture deposit. That same day, BOONE was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw \$500 from J.B.'s account at the drive-thru LFCU ATM located on West Mercury Boulevard in Hampton, Virginia. On January 29, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. On January 30, 2017, one counterfeit check was deposited into J.B.'s account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using J.B.'s debit card and PIN to withdraw \$500 from J.B.'s account at the walk-up ATM at the same LFCU branch located on West Mercury Boulevard in Hampton, Virginia.

21. On March 1, 2017, DICKERSON and BOONE were arrested by the Newport News Police Department, Hampton Police Division, and the United States Postal Inspection Service during a traffic stop in Hampton, Virginia. On that date, DICKERSON was observed

driving a 2009 Mercedes Benz, white in color, registered to DICKERSON through the Virginia Department of Motor Vehicles, with two other occupants. BOONE was identified as the sole rear-seat passenger, located immediately behind the driver. At the time of his arrest, DICKERSON was found with a stolen handgun loaded with a high-capacity magazine concealed in his waist band. Incident to arrest, the vehicle was searched for weapons immediately accessible to DICKERSON or the other passengers in the vehicle. A second handgun was found under the driver's seat, immediately accessible to BOONE. Inspection of the driver's seat revealed that the area from which this second handgun was recovered was not accessible from the driver's seat, only from the rear passenger seat, as a result of the motorized seat components. During the weapons sweep of the vehicle, investigators also observed credit/debit cards bearing names of individuals who were not in the vehicle. At that time, investigators stopped the search, maintained control of the vehicle, and applied for a state search warrant.

22. That same day, investigators executed a state issued search warrant on the vehicle described above. During the search, investigators located more credit/debit cards bearing names of individuals who were not in the vehicle; two counterfeit checks bearing the City of Norfolk seal and the name of a known accountholder; an HP laptop computer, model number 2000-410US; a printer; and numerous pages of blank check stock. Investigators also seized three cellular telephones: a black iPhone, Model A1778; and a pink iPhone, Model A1687; and a silver iPhone, Model A1549. The black and pink iPhones belonged to BOONE and the silver iPhone belonged to DICKERSON.

23. Based on information gathered from the investigation, investigators applied for and were issued a state search warrant for BOONE's residence located on Friendly Drive, in Hampton, Virginia. Investigators executed the search warrant on BOONE's residence on March

1, 2017. Inside the residence, investigators located and seized, among other items, two printers, an HP laptop computer, model Notebook 15-F233WM, hundreds of pages of blank check stock, numerous credit/debit cards in various names, counterfeit checks bearing the City of Norfolk seal and the name of the same known accountholder printed on the counterfeit checks found in DICKERSON's vehicle.

24. All of the items that were seized during the execution of the warrants on March 1, 2017 were packaged and placed into evidence at the Hampton Police Department. On April 27, 2017, these items were transferred to the United States Postal Inspection Service and placed into evidence, where they remain.

25. Based on the information obtained from the investigation and evidence recovered during the execution of the above-described warrants, BOONE and DICKERSON were both charged in Hampton, Virginia with 18.2-178 (Obtaining Money by False Pretense). BOONE was also charged with 18.2-308.2 (Possession of a Firearm by a Convicted Felon).

26. BOONE remained in stated custody after his arrest on March 1, 2017.

27. On March 9, 2017, DICKERSON was issued a bond in the Hampton, Virginia Court. DICKERSON posted bond later the same evening and was released from the Hampton, Virginia jail.

28. After his release, DICKERSON was identified in ATM surveillance images conducting additional transactions to access funds credited to accounts following remote capture deposits of worthless and counterfeit checks, including but not limited to the following transactions:

- a. On April 5, 2017, a counterfeit check was deposited into A.O.'s LFCU account via remote capture deposit. That same day, DICKERSON was captured by ATM surveillance equipment using A.O.'s debit card and PIN

attempting to withdraw \$500 from A.O.'s account at a walk-up ATM located on Jefferson Avenue in Newport News, Virginia.

- b. On April 12, 2017, DICKERSON was captured by ATM surveillance equipment depositing an altered Western Union money order into D.G.'s 1<sup>st</sup> Advantage Bank account. That same day, DICKERSON was again captured by ATM surveillance equipment using D.G.'s debit card and PIN as he withdrew \$100 from D.G.'s account at the drive-through ATM located at the 1<sup>st</sup> Advantage Bank on West Mercury Boulevard in Hampton, Virginia.

29. On April 12, 2017, a federal grand jury sitting in Newport News returned a 17-count indictment charging DICKERSON and BOONE with conspiring to commit bank fraud, in violation of 18 U.S.C. § 1349 (Count 1); bank fraud, in violation of 18 U.S.C. § 1344 (Counts 2-9); and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1) (Counts 10-16). The indictment also charged BOONE with possessing a firearm as a convicted felon, in violation of 18 U.S.C. § 922(g)(1) (Count 17).

30. On April 13, 2017, DICKERSON was pulled over in a traffic stop in Hampton, Virginia. On that occasion, DICKERSON was driving the same vehicle he had been operating on March 1, 2017. During the stop, DICKERSON was arrested on the outstanding federal arrest warrant. Incident to arrest, officers from the Hampton Police Division located on DICKERSON's person a black and silver Alcatel One Touch cellular telephone. After arresting DICKERSON, officers conducted an inventory of DICKERSON's 2009 Mercedes Benz prior to having it towed. During the inventory, officers located several debit cards within the passenger compartment, immediately accessible to the driver's seat. Two of the debit cards were in the names A.O. and D.G., accountholders whose accounts DICKERSON accessed after he was released on bond, as described above. Officers also located in the passenger compartment a white Samsung Galaxy Grand Prime cellular telephone, as well as a printer and blank check stock.

31. All of the items that were recovered from the inventory of DICKERSON's vehicle were turned over to Newport News Police Detective and U.S. Postal Inspection Service Task Force Officer (TFO) E. Benson. These items were entered into to Newport News Property and Evidence, where they currently remain.

32. DICKERSON made his initial appearance on April 14, 2017. Boone made his initial appearance on June 2, 2017. Trial is currently set for September 6, 2017.

#### LEGAL AUTHORITY

33. The legal authority for this search warrant application regarding the Instagram Inc. accounts described in Attachment A is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

34. 18 U.S.C. § 2703(b) provides in relevant part as follows:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

...

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –

RJK

- (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
- (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

35. The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. Title 18, United States Code, Sections 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

36. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated herein. As part of this investigation, Newport News Police Detective E. Benson has sent preservation requests to Instagram pursuant to 18 U.S.C. § 2703(f), requiring Instagram to maintain the contents of the account(s) associated with usernames “bigmoney\_jordan,” “freebandkid23,” and “freebandswervo.” These requests were sent on January 13, 2017; January 27, 2017; and February 16, 2017, respectively.

#### DEFINITIONS

37. The term “computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data

processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

38. The terms “records,” “documents,” and “materials” include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

- a. documents, spreadsheets, records or representations;
- b. photographs;
- c. pictures;
- d. images, and
- e. aural records or representations.

39. The terms “records,” “documents,” and “materials” include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

40. The term “Universal Resource Locator” (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

41. The term “Internet Protocol Address” (IP Address): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses; static and dynamic. A static address is permanent and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

42. The term “Internet Service Providers” (ISPs): Individuals who have an Internet account and an Internet-based electronic mail (e-mail) address must have a subscription, membership, or affiliation with an organization or commercial service which provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or “ISP”.

43. A “MAC Address” refers to the fact that every computer has a unique identifying number that is placed there by the manufacturer. It is based upon a set standard that all manufacturers have agreed upon, and no two MAC Addresses are alike. A MAC Address is similar to the VIN number of a vehicle, as the number is not changeable.

44. “Web hosts” provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is “shared,” which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. “Dedicated hosting,” means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. “Co-location” means a server is located at a dedicated

hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

45. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

46. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

47. "Electronic Communications System" means any wire, radio, electromagnetic, photo optical, or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

48. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

49. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

## **TECHNICAL BACKGROUND**

50. From my review of publicly available information provided by Instagram about its service, including Instagram's "Privacy Policy," I am aware of the following about Instagram and about the information collected and retained by Instagram. Instagram owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.instagram.com>.

51. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application ("app") created by the company that allows users to access the service through a mobile device.

52. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add a caption to the photo, can add various "tags" to the photo that can be used to search for the photo (e.g., a user made add the tag #vw to a photo so that people interested in Volkswagen vehicles can search for and find the photo), can add location information to the photo, and can add other information to photo, as well as apply a variety of "filters" or other visual effects that can be used to modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also "like" photos.

53. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by

PJL

Instagram. A user may change the username and/or password at any point while still maintaining the original account and all information contained therein.

54. Instagram asks users to provide basic identity and contact information upon registration and allows users to provide additional identity information for their user profile. This information may include the user's full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. This information is collected and maintained by Instagram.

55. Instagram allows users to have "friends," that is, other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contacts lists maintained by the user, other third-party social media websites, and information or searches conducted by the user on Instagram profiles. This information is collected and maintained by Instagram.

56. Instagram also allows users to "follow" another user, which means that they receive updates about posts made by the other user. Users may also "unfollow" other users, that is, stop following the other user. Users may also block other users, which prevents the other users from following them.

57. Instagram allow users to post and share various types of user content, including photos, comments, and other materials. User content that is posted to Instagram or shared through Instagram is collected and maintained by Instagram.

58. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

59. For each user, Instagram also collects and retains information, called “log file” information, associated with every time a user requests access to Instagram, whether through a web page or through an app. The log file information that Instagram’s servers automatically records includes the particular web requests, any Internet Protocol (“IP”) address associated with the request, the type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

60. Instagram also collects and maintains “cookies,” which are small text files that are placed on a user’s computer or mobile device and that allow Instagram to identify the browser or device’s accessing the service.

61. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record “device identifiers,” which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

62. Instagram also collects metadata associated with user content. For example, Instagram collects any “hashtags” associated with user content (i.e., keywords used), “geotags” that mark the location of a photo and may include latitude and longitude information, comments on photos, and other information.

63. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

64. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the Instagram account(s) associated with the usernames “bigmoney\_jordan” and/or “freebandkid23” and/or “freebandswervo,” including stored electronic communications and information concerning subscribers and their use of

Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

### **SEARCH PROCEDURES**

65. The search warrant will be sent electronically via the Instagram Law Enforcement Online Requests portal to personnel with Instagram who will be directed to produce the information noted in the warrant. Consistent with the procedures outlined in Attachment B, your affiant and other agents will review the production and seize those e-mails and/or records that are authorized by the search warrant.

### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

66. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Instagram to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

67. Based on the forgoing, I submit that probable cause exists to believe that the users of the Instagram account(s) associated with the usernames “bigmoney\_jordan” and/or “freebandkid23” and/or “freebandservvo,” believed to be Markis DICKERSON have violated 18 U.S.C. § 1349 (Conspiracy to Bank Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft), and that probable cause exists to believe that

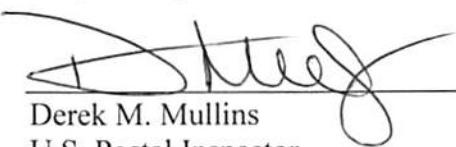
evidence, fruits, and instrumentalities of such violations will be found within the information associated with such Instagram account(s).

68. Accordingly, I request that warrants be issued authorizing the United States Postal Inspection Service, with assistance from other law enforcement personnel, to search those premises noted in Attachment A and obtain the information in the accounts for the items noted in Attachment B.

69. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

70. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Instagram accepts out-of-state and out-of-district service of subpoenas, court orders, and search warrants via the Law Enforcement Online Requests portal without the presence of a law enforcement officer. Accordingly, your affiant will execute the requested search warrant by e-mail to the custodian of records at Instagram and permission is requested for the data to be copied / obtained outside of the presence of a law enforcement officer. It is anticipated that Instagram will produce the requested records in electronic format accompanied by a signed authentication letter via E-mail or on electronic media via U.S. Mail to your affiant.

Respectfully submitted,

  
\_\_\_\_\_  
Derek M. Mullins  
U.S. Postal Inspector  
U.S. Postal Inspection Service

This affidavit has been reviewed for legal sufficiency by:

Kaitlin C. Gratton

Kaitlin C. Gratton

Assistant United States Attorney

Subscribed and sworn to before me this 9<sup>th</sup> day of June, 2017, in the City of Norfolk, Virginia.

Robert J. Stark  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Instagram account(s) associated with usernames:

- (1) "bigmoney\_jordan,"
- (2) "freebandkid23," and
- (3) "freebandservvo"

which is stored at premises owned, maintained, controlled, or operated by Instagram, a social-networking company headquartered in San Francisco, California and owned by Facebook, Inc., a social-networking company headquartered in Menlo Park, California.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Instagram**

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram, including any messages, records, files, logs, or information that has been deleted but is still available to Instagram, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram is required to disclose the following information to the government for each account listed in Attachment A:

- a. All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Instagram passwords, Instagram security questions, physical address (including city, state, and zip code), telephone numbers, screen and user names, websites, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All log file information, including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;
- e. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie

information, including all information about the particular device or devices used to access the account and the date and time of those accesses;

- f. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- g. All communications or other messages sent or received by the account;
- h. All user content created, uploaded, shared, or accessed by the account, including any comments made by the account on photographs or other content;
- i. All photographs and images in the user gallery for the account;
- j. All location data associated with the account, including geotags;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list), as well as any friends of the user;
- m. A list of all users that the account has “unfollowed” or blocked;
- n. All privacy and account settings;
- o. All records of Instagram searches performed by the account, including all past searches saved by the account;
- p. All information about connections between the account and third-party websites and applications;
- q. All records pertaining to communications between Instagram and any person regarding the user or the user’s Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. §1028A(a)(1) (Aggravated Identity Theft), those violations involving Markis DICKERSON and other co-conspirators occurring after **August 1, 2014**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications and any account content and information involving and concerning the recruitment and solicitation of accountholders;
- b. Communications and any account content and information about or reflecting the recruitment process;
- c. Communications among known and unknown co-conspirators;
- d. Preparatory steps taken in furtherance of the fraud scheme;
- e. Records of association, including follower/following lists and follower requests among conspirators and accountholders, presently known and unknown;
- f. All profile information, account content and information, and communications relating to violations of 18 U.S.C. § 1349 (Conspiracy to Commit Bank Fraud); 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1028A(a)(1) (Aggravated Identity Theft); and
- g. Records relating to who created, used, accessed, or communicated with the account, including any records about their identities and whereabouts.